

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

MICHAEL J. NEWMAN

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Information associated with the Instagram account name  
bigblue8992 that is stored at premises controlled by  
Instagram LLC

Case No.

**3 : 17 mj 227**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A-4located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C-4

Offense Description

The application is based on these facts:  
See Attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

FILED  
 RICHARD W. NAGEL  
 CLERK OF COURT  
 2017 MAY 22 PM 3:33  
 U.S. DISTRICT COURT  
 SOUTHERN DIST. OHIO  
 WESTERN DIV. DAYTON

Andrea R. Kinzig  
 Applicant's signature

Andrea R. Kinzig, Special Agent  
 Printed name and title

Sworn to before me and signed in my presence.

Date:

5/22/17City and state: Dayton, Ohio

Michael J. Newman  
 Judge's signature

Michael J. Newman, U.S. Magistrate Judge  
 Printed name and title

**ATTACHMENT A-4**

**Property to Be Searched**

Information associated with the Instagram account name **bigblue8992** (located at <https://www.instagram.com/bigblue8992/>) that is stored at premises owned, maintained, controlled, or operated by Instagram LLC, a company that accepts service of legal process at 1601 Willow Road, Menlo Park, California, 94025.

**ATTACHMENT B-4**

**Particular Things to be Seized**

**I. Information to be disclosed by Instagram LLC (the “Provider”)**

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-4:

- (a) All contact information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All Photoprints, including all photos uploaded by the user ID and all photos uploaded by any other tagged user;
- (c) All Neoprints, including profile contact information; Mini-Feed information; links to videos, photographs, articles, and other items; Notes; Friends lists, including the friends’ Instagram user identification number; Groups and networks of which the user is a member, including groups’ Instagram group identification numbers; Rejects “Friend” requests; comments; Gifts; Tags; and information about the user’s access and use of Instagram application;
- (d) All other communications and messages made or received by the user, including all private messages and pending “Friend” requests;
- (e) All IP logs, including all records of the IP addressed that logged into the account;
- (f) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
- (g) All privacy settings and other account settings;
- (h) All records pertaining to communications between Instagram and any person regarding the use of the user’s Instagram account, including contacts with support services and records of actions taken.

Pursuant to the warrant, Instagram LLC shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or by making the data available to the Federal Bureau of Investigation via Instagram LLC’s electronic portal.



## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of the offenses advertisement of child pornography, in violation of 18 U.S.C. § 2251(d); receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1) and 2252A(a)(2); transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1); possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) and 2252A(a)(5)(B); and committing a felony offense involving a minor while being required to register as a sex offender, in violation of 18 U.S.C. § 2260A, involving the user of the account and occurring from March 1, 2015 to the present, including, for each account or identifier listed on Attachment A-4, information pertaining to the following matters:

- a. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
- b. Any visual depictions of minors;
- c. Any communications with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;
- d. Any communications with minors, and any contact / identifying information for these minors;
- e. Evidence of utilization of email accounts, social media accounts, online chat programs, and file storage accounts, including any account / user names;
- f. Any information regarding utilization of websites and social media sites to access or obtain child pornography, communicate with juveniles, or communicate with others regarding child exploitation offenses;
- g. Evidence of utilization of aliases and fictitious names;
- h. Any information related to Internet Protocol (IP) addresses accessed by the account;
- i. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.



**ATTACHMENT C-4**

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252(a)(1)	Transportation of Child Pornography
18 U.S.C. §2251(d)	Advertisement of Child Pornography
18 U.S.C. §2260A	Committing a Felony Offense Involving a Minor While Being Required to Register as a Sex Offender

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, advertisement, distribution, receipt, transportation, and possession of child pornography. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review thousands of examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents and investigators from the FBI, I am currently involved in an investigation of child pornography offenses committed by a suspect identified as JASON BIGLER. This Affidavit is submitted in support of Applications for search warrants for the following:
  - a. Information associated with the email account **amandabigs@yahoo.com** that is stored at premises controlled by Yahoo Inc. (as more fully described in Attachment A-1);
  - b. Information associated with the Facebook accounts associated with the email addresses **bigblue8992@yahoo.com** and **amandabigs@yahoo.com** that is stored at premises controlled by Facebook Inc. (as more fully described in Attachment A-2);
  - c. Information associated with the Twitter account **@bigblue8992** that is stored at premises controlled by Twitter Inc. (as more fully described in Attachment A-3);
  - d. Information associated with the Instagram account name **bigblue8992** that is stored at premises controlled by Instagram LLC (as more fully described in Attachment A-4).
3. The purpose of the Applications is to seize evidence of the following violations: advertisement of child pornography, in violation of 18 U.S.C. § 2251(d); receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1) and 2252A(a)(2); transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1); possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) and 2252A(a)(5)(B); and committing a felony offense involving a minor while being required to register as a sex offender, in violation of 18 U.S.C. § 2260A. The items to be searched for and seized are described more particularly in Attachments B-1 through B-4 hereto.

4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 through A-4).
6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1), 2252A(a)(2), 2252(a)(1) & (b)(1), 2252(a)(4)(B) & (b)(2), 2252A(a)(5)(B), 2251(d), and 2260A, are present in the above noted accounts (as described in Attachments A-1 through A-4).

### **JURISDICTION**

7. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PERTINENT FEDERAL CRIMINAL STATUTES**

8. 18 U.S.C. § 2251(d) states that it is a violation for (1) any person to knowingly make, print, or publish, or cause to be made, printed, or published, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct; (2) if such person knows or has reason to know that such notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed.
9. 18 U.S.C. § 2252(a)(1) and (b)(1) states that it is a violation for any person to knowingly transport or ship using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.



10. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mail if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
11. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
12. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
13. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
14. 18 U.S.C. § 2260A states that whoever, being required by Federal or other law to register as a sex offender, commits a felony offense involving a minor shall be sentenced to a term of imprisonment of ten years in addition to the imprisonment imposed for the offense under that provision.
15. For purposes of the statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:
  - a. “Actual or simulated –

- i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- ii. Bestiality;
- iii. Masturbation;
- iv. Sadistic or masochistic abuse; or
- v. Lascivious exhibition of genitals or pubic area of any person.”

### **BACKGROUND INFORMATION**

#### **Definitions**

16. The following definitions apply to this Affidavit and Attachments B-1 through B-4:

- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can



establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

- f. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. “**Hyperlink**” (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- h. “**Website**” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- i. “**Uniform Resource Locator**” or “**Universal Resource Locator**” or “**URL**” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- j. A “**Zip file**” is an archive file format that supports lossless data compression. A Zip file may contain one or more files or directories that may have been compressed.



Collectors of Child Pornography

17. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
  - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
  - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
  - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
  - e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
  - f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Cloud Storage and Dropbox

18. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:
- a. “Cloud” is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. “The cloud” was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.
  - b. “Cloud computing” is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
  - c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSP’s offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP’s maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP’s reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.” CSP’s may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.



- d. “Virtual Machine” (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.
  - e. “NetFlow Records” are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.
19. Dropbox is an on-line file hosting service operated by Dropbox Inc., a company headquartered in San Francisco, California. Dropbox accounts provide users with cloud storage, file synchronization, personal cloud, and client software. Dropbox creates a special folder on the user’s computer, and the contents of the folder are synchronized to Dropbox Inc.’s servers and to other computers and devices onto which the user has installed Dropbox, keeping the same files up-to-date on all devices. Users are provided 2 GB of free storage space for basic accounts.
20. Dropbox Inc. provides its users with the ability to share files or folders with others, including individuals who do not have Dropbox accounts. One means of sharing files or folders is by creating a “sharing link”. A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

#### Email Accounts

21. Yahoo Inc. allows subscribers to obtain e-mail accounts at the domain names yahoo.com, like the account listed in Attachment A-1. Subscribers obtain an account by registering with Yahoo Inc. During the registration process, Yahoo Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo Inc. subscribers) and information concerning subscribers and their use of Yahoo Inc. services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.



22. A Yahoo Inc. subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Yahoo Inc. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.
23. E-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
24. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.
25. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

#### Facebook

26. Facebook Inc. (hereinafter referred to as "Facebook") owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

27. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.
28. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.
29. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.
30. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.
31. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user.



that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

32. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.
33. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.
34. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.
35. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.
36. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.
37. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.
38. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.
39. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.



40. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.
41. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.
42. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
43. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.
44. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the

physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

### Twitter

45. Twitter Inc. (hereinafter referred to as “Twitter”) owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.
46. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.
47. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user’s full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user’s profile was created, the date and time at which the account was created, and the Internet Protocol (“IP”) address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.
48. A Twitter user can post a personal photograph or image (also known as an “avatar”) to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post “bios” of 160 characters or fewer to their profile pages.
49. Twitter also keeps IP logs for each user. These logs contain information about the user’s logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.



50. As discussed above, Twitter users can use their Twitter accounts to post “Tweets” of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also “favorite,” “retweet,” or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have favorited or retweeted the user’s own Tweets, as well as a list of all Tweets that include the user’s username (*i.e.*, a list of all “mentions” and “replies” for that username).
51. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.
52. Twitter users can also opt to include location data in their Tweets, which will reveal the users’ locations at the time they post each Tweet. This “Tweet With Location” function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.
53. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter’s link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.
54. A Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user’s “followers” list) and a list of people whom that user follows (*i.e.*, the user’s “following” list). Twitter users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into “lists” that display on the right side of the user’s home page on Twitter. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.
55. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter’s database.
56. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user’s mobile phone, and the user can also set up a “sleep time” during which Twitter updates will not be sent to the user’s phone.



57. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.
58. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.
59. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.
60. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.
61. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

#### Instagram

62. Instagram LLC (hereinafter referred to as "Instagram") provides users with an online photo-sharing and social networking service that enables users to take pictures, apply digital filters to them, and share them on a variety of social networking services, such as Facebook or Twitter. A distinctive feature is that it confines photos to a square shape, similar to Kodak Instamatic and Polaroid images, in contrast to the 16:9 aspect ratio now typically used by mobile device cameras.
63. Instagram asks users to provide basic contact and personal identifying information to Instagram, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email address, Instagram passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Instagram also assigns a user identification number to each account.
64. Instagram users can select different levels of privacy for the communications and information associated with their Instagram accounts. By adjusting these privacy settings, and Instagram user can make information available only to himself or herself, to particular Instagram users, or to anyone with access to the Internet, including people who are not Instagram users.

65. Instagram users can post comments on the Instagram profiles of other users or on their own profiles. Such comments are typically associated with a specific posting or item on the profile. These chat communications are stored in the chat history for the account.
66. Instagram has a “like” feature that allows users to give positive feedback. Instagram users can “like” Instagram photos or posts. They can also post comments to these photos and posts.
67. Each Instagram account has an activity log, which is a list of the user’s posts and other Instagram activities from the inception of the account to the present. The activity log includes the photos and the posts or comments other users have made in regards to those photos and posts.
68. Instagram also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Instagram, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views an Instagram profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
69. Social networking providers like Instagram typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of services utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Instagram users may communicate directly with Instagram about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Instagram typically retain records about such communications, including records of contacts between the user and the provider’s support devices, as well as records of any actions taken by the provider or user as a result of the communications.
70. Therefore, the computers of Instagram are likely to contain all of the material described above, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, transaction information, and other account information.

#### Background on NCMEC

71. The National Center for Missing and Exploited Children (commonly known as “NCMEC”) was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
72. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding



suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

### **BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE**

#### **CyberTipline Reports**

73. On or around September 15, 2016, an anonymous citizen reported to NCMEC's CyberTipline that child pornography was located at the following URL: <https://www.dropbox.com/sh/zdvrd4evmkaenkj/AABC7UPVDMI5eztCvrmYYDzSA?dl=0>. A CyberTipline report was prepared and forwarded to the FBI for further investigation.
74. On or around September 21, 2016, an FBI analyst accessed the aforesaid URL and found that it contained a Dropbox sharing link to approximately thirty-seven image files, some of which contained child pornography. The analyst downloaded the thirty-seven files and provided them to me for further review. Based on my training and experience, I believe that at least approximately fifteen of the files depict images of child pornography (as defined by 18 U.S.C. § 2256). Two of the files are described as follows:
  - a. A file entitled "5393e6e9-13f0-4789-9422-a3029f0d43dd.jpg" is an image that depicts a pre-pubescent white female child who is completely nude. The child is squatting over an object that is inserted into her vagina.
  - b. A file entitled "63337ca7-6610-4b98-be23-963184cc94b5.jpg" is an image that depicts the groin area of what appears to be an infant white female child. The penis of what appears to be an adult white male is touching the child's nude vagina.
75. On or around September 21, 2016, an administrative subpoena was served on Dropbox Inc. requesting information associated with the aforesaid Dropbox URL. Records provided by Dropbox Inc. in response to this subpoena identified that the URL belonged to a Dropbox account held in the name of "Jay Bigs", with a log-in email address of [bigblue8992@yahoo.com](mailto:bigblue8992@yahoo.com). Dropbox Inc.'s records further indicated that the user had established the account on or around June 30, 2016. Dropbox Inc.'s records also identified that the account had been logged into on two occasions<sup>1</sup> – that being on June 30, 2016 and September 1, 2016. According to Dropbox Inc.'s records, the IP address of 50.5.114.147 was utilized to access the account on both occasions.
76. On or around October 4, 2016, Dropbox Inc. reported to NCMEC's CyberTipline that approximately fifteen image files and approximately six video files containing suspected child pornography were discovered in the publicly available or shared content of the

---

<sup>1</sup> Based on its law enforcement guide, Dropbox Inc. only maintains logs of IP addresses for a period of six months. The guide also notes that IP addresses are only captured by Dropbox Inc. when a user logs into the account through the Dropbox website. If users access their accounts through desktop or mobile applications, that access may not be logged by Dropbox Inc.



Dropbox account with an account name of “Jay Bigs” and with a log-in email address of **bigblue8992@yahoo.com** (the same account noted above that contains the aforesaid sharing link). Dropbox Inc. provided NCMEC with the twenty-one image and video files as well as other account information. The files and account information were forwarded to the FBI for further investigation.

77. I have reviewed the twenty-one files provided by Dropbox Inc. I noted that many of these files are the same as those downloaded by the FBI analyst on or around September 21, 2016, including the two image files described in paragraph 77. Based on my training and experience, I believe that at least fifteen of the image files and at least six of the video files provided by Dropbox Inc. depict child pornography (as defined by 18 U.S.C. § 2256). One of the files is described as follows:

- a. A file entitled “5e12d91e-9e45-4ee1-8bdc-b078ddd00440.mp4” is a video that depicts two pre-pubescent white female children, one of whom is nude and the other of whom is wearing clothing. The child who is wearing clothing is inserting an object into the vagina of the nude child. The video is approximately thirty-one seconds in duration.

Records Received Pursuant to Subpoenas and Search Warrants

78. Cincinnati Bell was identified as the Internet Service Provider of the IP address 50.5.114.147 (the IP address utilized to log into the **bigblue8992@yahoo.com** Dropbox account, as detailed above). On or around October 24, 2016, an administrative subpoena was served on Cincinnati Bell requesting subscriber information for this IP address on the aforesaid two dates and times it was used to log into the subject Dropbox account. Records provided by Cincinnati Bell in response to the subpoena identified that this account was subscribed to in the name of Lois Bigler at 104 Virginia Avenue in Dayton, Ohio. Lois Bigler’s Internet account was created on or around May 7, 2016, and it remained active as of the date of the subpoena.
79. During the course of the investigation, the IP address of 50.5.120.177 was also identified as being used by various accounts (as detailed below). On or around May 17, 2017, an additional administrative subpoena was served on Cincinnati Bell requesting subscriber information for this IP address on a sample of the dates and times it was used to access the subject accounts. Records provided by Cincinnati Bell in response to the subpoena identified that this IP address was also subscribed to Lois Bigler’s Internet account at 104 Virginia Avenue in Dayton, Ohio.
80. On or around December 29, 2016, an administrative subpoena was served on Yahoo Inc. requesting information for the **bigblue8992@yahoo.com** email account. Records provided by Yahoo Inc. in response to the subpoena identified that the account was created on or around March 1, 2015, and that the user identified his name as being “J Big” (which is similar to the “Jay Bigs” name associated with the **bigblue8992@yahoo.com** Dropbox account). The user also provided a telephone number of 937-304-4995 as an alternate communication channel.

81. Sprint Corporation was identified as being the service provider for telephone number 937-304-4995. On or around January 6, 2017, an administrative subpoena was served on Sprint Corporation requesting subscriber and transactional information for this phone number for the time period of July 1, 2016 to January 6, 2017. Records received from Sprint Corporation in response to the subpoena identified that this account was subscribed to in the name of Lois Bigler, with a billing address of 104 Virginia Avenue in Dayton, Ohio. Records also identified that the telephone associated with the account had accessed Internet data on approximately thirty-three occasions between the approximate time period of October 28, 2016 and January 30, 2017.
82. On or around February 6, 2017, an administrative subpoena was served to Google, Inc. requesting information for any Google accounts associated with the email address **bigblue8992@yahoo.com**. Records provided by Google Inc. in response to the subpoena identified that the **bigblue8992@yahoo.com** email address was associated with a Google account using the email address **bigblue8992@gmail.com**.
83. In February 2017, the United States District Court for the Southern District of Ohio authorized search warrants for the following:
  - a. Information associated with the account **bigblue8992@gmail.com** that is stored at premises controlled by Google Inc. (to include contents of the email account);
  - b. Information associated with the account **bigblue8992@yahoo.com** that is stored at premises controlled by Yahoo Inc. (to include contents of the email account);
  - c. Information associated with the Dropbox account **bigblue8992@gmail.com** that is stored at premises controlled by Dropbox Inc. (to include contents of the Dropbox account);
  - d. Information associated with the Dropbox account **bigblue8992@yahoo.com** that is stored at premises controlled by Dropbox Inc. (to include contents of the Dropbox account);
84. The search warrants were served on Google Inc., Yahoo Inc., and Dropbox Inc. in February 2017.
85. Google Inc. provided records in response to the search warrant for the **bigblue8992@gmail.com** account in February 2017. Review of the records provided the following information:
  - a. The **bigblue8992@gmail.com** email account was created on or around April 6, 2015 in the name of "A Big". Google Inc.'s records identified that the account user's telephone number was 937-304-4995 (the same telephone number listed as an alternate communication channel for the **bigblue8992@yahoo.com** email account and that is subscribed to Lois Bigler at 104 Virginia Avenue in Dayton,



Ohio, as detailed above) and that his alternate email address was **bigblue8992@yahoo.com**.

- b. Google Inc.'s records identified that the account user logged into the email account on approximately eight occasions during the approximate time period of September 22, 2016 to February 8, 2017. The IP addresses of 50.5.114.147 and 50.5.120.177 (both of which are subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above) were utilized to log into the account on each of these occasions.
  - c. The user of the email account had received a number messages from email addresses associated with the Dropbox Inc. and pCloud LTD<sup>2</sup> companies. These messages indicated that the **bigblue8992@gmail.com** email account user had cloud storage accounts with both companies.
  - d. Google Inc. maintains Internet search histories for users that use a "Web and App Activity" service provided by Google Inc. For users that use this service, Google Inc. maintains search queries and results when the users conduct searches while logged into their Google accounts. Google Inc.'s records indicated that the **bigblue8992@gmail.com** account user conducted the following searches on or around April 6, 2015: "young naked", "preteen naked", "preteen nonude", and "preteen". Based on my training and experience, I know that these terms are commonly used by individuals to search for child pornography and child erotica.
86. Dropbox Inc. provided records in response to the search warrant for the **bigblue8992@yahoo.com** account in April 2017. Review of these records provided the following information:
- a. The account was held in the name of "Jay Bigs", with a log-in email address of **bigblue8992@yahoo.com**. The account was established on or around June 30, 2016.
  - b. A log of IP addresses<sup>3</sup> utilized to access the account identified that the account had been logged into on one occasion on or around September 1, 2016. The IP address of 50.5.114.147 (the IP address subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above) was utilized to log into the account on this date.
  - c. What was identified as an "iPad3,4" was utilized to access the Dropbox account on one occasion on September 22, 2016.

---

<sup>2</sup> pCloud is cloud storage service provided by pCloud LTD, a company based in Switzerland.

<sup>3</sup> As previously noted, Dropbox Inc. only maintains logs of IP addresses for a period of six months and for users who log into their accounts through the Dropbox website. Given that more than six months had passed, the records received in response to the search warrant did not capture the log-in on June 30, 2016, that was reported on the records received in response to the administrative subpoena (as detailed in paragraph 19).



- d. Approximately 790 image and video files were saved in the account as of the date that Dropbox Inc. preserved records for the account pursuant to a preservation request made by the FBI in December 2016. The files were saved in eleven folders. Review of the files identified that they nearly all contained images and videos of children, teenagers, and young adults, many of whom were engaged in sexually explicit conduct. These files included the files downloaded by the NCMEC analyst on or around September 21, 2016 (as detailed in paragraph 18) and the files provided by Dropbox Inc. pursuant to the CyberTipline Report (as detailed in paragraphs 20 and 21). Based on a preliminary review of the files, I believe that more than one hundred and fifty of the image files and more than fifty-five of the video files depict child pornography (as defined by 18 U.S.C. § 2256). Two of the files are described as follows:
    - i. A file entitled “ba93beb4-2858-4e92-8690-3effe183ec8f.jpg” is an image that depicts a pre-pubescent white female child who is nude and lying on her back with her legs spread apart. The words “FUCK ME” are written above the child’s vagina, and there is an arrow pointing to her vagina. The penis of what appears to be an adult white male is inserted into the child’s vagina. The penis of what appears to be another adult white male is next to the child’s face. The file was saved in a folder entitled “Young”.
    - ii. A file entitled “pedomom quick pussy lick1m.mp4” is a video that depicts a pre-pubescent white female child who is nude and lying on her back with her legs spread apart. What appears to be an adult white female is licking the child’s vagina. The file was saved in a folder entitled “mom”.
  - e. A file activity log provided by Dropbox Inc. for the account identified that each of the files described above in paragraph 86(d) as well as the video file described in paragraph 77 (which was provided by Dropbox Inc. pursuant to the CyberTipline report) were uploaded to the Dropbox account on or around August 31, 2016.
  - f. Approximately eight sharing links were created by the account user. These sharing links included the link reported to NCMEC’s CyberTipline from which the NCMEC analyst accessed and downloaded files, as described in paragraphs 73 and 74.
87. On or around April 27, 2017, I attempted to access the aforesaid sharing links that were posted by the user of the bigblue8992@yahoo.com Dropbox account user (i.e., the links referenced in paragraph 86(f)). These links were no longer active on this date.
88. Dropbox Inc. provided records in response to the search warrant for the bigblue8992@gmail.com account in April 2017. Review of these records provided the following information:

- a. The account was held in the name of "J A", with a log-in email address of bigblue8992@gmail.com. The account was established on or around January 11, 2017.
- b. A log of IP addresses utilized to access the account identified that the account had been logged into on approximately four occasions during the approximate time period of January 11, 2017 to February 9, 2017. The IP address of 50.5.120.177 (the IP address that is subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above) was utilized to log into the account on each of these occasions.
- c. What was identified as an "iPad3,4" was utilized to access the Dropbox account on two separate dates.
- d. Thousands of image, video, and Zip files were saved in the account as of the date that Dropbox Inc. preserved records for the account pursuant to a preservation request made by the FBI in February 2017. The files were saved in a folder called "for angie". Some of these files were password protected, and as such, could not be accessed. Review of the remaining files identified that they nearly all contained images and videos of children, teenagers, and young adults in various states of undress, many of whom were engaged in sexually explicit conduct. Based on a preliminary review of the files, I believe that more than two thousand of the image files and more than eighty of the video files depict child pornography (as defined by 18 U.S.C. § 2256). Three of the files are described as follows:
  - i. A file entitled "4yo Sleepy Time = June 10, 2005 016.jpg" is an image that depicts a pre-pubescent white female child who is nude and has her legs spread apart. The penis of what appears to be an adult white male is partially inserted into the child's vagina. The file was saved in a Zip file entitled "Bunny.zip". This Zip file contained approximately twenty-four image files, at least approximately seventeen of which depict child pornography.
  - ii. A file entitled "040.jpg" is an image that depicts a pre-pubescent white female child performing oral sex on what appears to be a dog's penis. The file was saved in a Zip file entitled "M\_1.zip". This Zip file contained approximately three hundred and eighty image files, at least approximately sixty-nine of which depict child pornography.
  - iii. A file entitled "4.flv" is a video that depicts a nude pre-pubescent white female child whose legs are bound over her head with a white material. What appears to be a nude adult white male inserts his penis into the child's buttocks and vagina and secretes semen on her abdomen. The video is approximately two minutes and one second in duration. The file was saved in a Zip file entitled "norm.zip". This Zip file contained approximately ten video files, all of which depict child pornography.



- e. A file activity log provided by Dropbox Inc. for the account identified that each of the files described above in paragraph 88(d) were uploaded to the Dropbox account on or around January 11, 2017.
  - f. One sharing link was created by the account user.
89. On or around April 20, 2017, I accessed the aforesaid sharing link that was posted by the user of the bigblue8992@gmail.com Dropbox account (i.e., the sharing link identified in paragraph 88(f)). I found that the website contained hyperlinks to approximately 539 image, video, Zip, and HTML files that were saved in a folder called “for angie”. It appears that these files are the same as many of those contained in the bigblue8992@gmail.com Dropbox account. I selected three Zip files entitled “Bunny.zip”, “M\_1.zip”, and “norm.zip” from this website and successfully downloaded them. I noted that the contents of these Zip files were the same as those provided by Dropbox Inc. for the bigblue8992@gmail.com account and that are described above in paragraph 88(d).
90. Yahoo Inc. provided records in response to the search warrant for the bigblue8992@yahoo.com account in May 2017. Review of these records provided the following information:
- a. The bigblue8992@yahoo.com email account was created on or around March 1, 2015 in the name of “J Big”. According to Yahoo Inc.’s records, the user identified during the registration process that his birth date was May 7, 1971. Yahoo Inc.’s records also identified that the user’s alternate communication channel was telephone 937-304-4995 (the same telephone number listed for the bigblue8992@gmail.com email account and that is subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above).
  - b. Yahoo Inc.’s records identified that the account user logged into the email account on approximately forty-seven occasions during the approximate time period of May 22, 2016 to February 7, 2017. The IP addresses of 50.5.114.147 and 50.5.120.177 (both of which are subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above) were utilized to log into the account on approximately forty-six occasions.
  - c. The user of the email account had received a number messages from email addresses associated with the Dropbox Inc. and pCloud LTD<sup>4</sup> companies. These messages indicated that the bigblue8992@yahoo.com email account user had cloud storage accounts with both companies.
  - d. Numerous email messages were recovered that included JASON BIGLER’s name in the content of the messages, photographs of JASON BIGLER attached to the messages, and messages in which the account user identified that his telephone number was 937-304-4995.

---

<sup>4</sup> pCloud is cloud storage service provided by pCloud LTD, a company based in Switzerland.

- e. Various email messages were received by the **bigblue8992@yahoo.com** account indicating that the email address was associated with accounts on various websites, including Facebook, Instagram, and Twitter.
- f. Approximately thirty-six email messages were recovered from the account that were sent or received by the email address **amandabigs@yahoo.com**. The **bigblue8992@yahoo.com** account was not listed as a recipient or sender of these messages. Based on my training and experience, I know that individuals can automatically forward or re-direct email messages from one account to another by adjusting their account settings. Based on the context of these messages, the use of the name “bigs” in the **amandabigs@yahoo.com** email address, and other information noted in this Affidavit, I submit that it is reasonable to believe that the same individual uses the **amandabigs@yahoo.com** and **bigblue8992@yahoo.com** email addresses. Further review of the email messages sent to or from the **amandabigs@yahoo.com** email account provided the following information:
  - i. A number of messages were exchanged between **amandabigs@yahoo.com** and another individual in which the two users discussed the possibility of meeting to engage in sexual activities. It appeared that the **amandabigs@yahoo.com** account user was representing him/herself as a juvenile. In other messages, it appeared based on the context of the messages that the two account users were discussing videos that contained sexually explicit conduct of one or more juveniles.
  - ii. One message was received by the **amandabigs@yahoo.com** account that contained a photograph of a juvenile female child attached to it. The child was wearing clothing in the photograph.
  - iii. Approximately five messages were received by the **amanadabigs@yahoo.com** account that indicated that the account user had an account on the Facebook website.

Background on JASON BIGLER and Lois Bigler

- 91. The investigation determined that Lois Bigler is approximately seventy-four years of age and is the mother of JASON BIGLER. JASON BIGLER’s date of birth is May 7, 1971 (the same date of birth listed in the subscriber information for the **bigblue8992@yahoo.com** email account). Records from the Montgomery County Sheriff’s Office identified that JASON BIGLER is currently required to register as a sex offender as a result of two prior convictions in May 2002 and June 2007 (as further detailed below). Review of various police reports and court records revealed the following information:



- a. In September 2000, JASON BIGLER was arrested by the Grove City (Ohio) Police Department for rape, in violation of Ohio Revised Code Section 2902.02. Records from the Grove City Police Department identified that a 14-year old female child reported that JASON BIGLER had engaged in sexually explicit conduct with her after meeting her on the Internet. The child further reported that when they first began communicating with each other, JASON BIGLER represented himself as being 16 years old. The criminal charges were later dismissed.
  - b. In May 2002, JASON BIGLER was convicted in the Van Wert County (Ohio) Common Pleas Court of one count of unlawful sexual conduct with a minor, in violation of Ohio Revised Code Section 2907.04(a). JASON BIGLER was sentenced to two years imprisonment. Based on records from the Adult Parole Authority of the Ohio Department of Rehabilitations and Corrections, I have determined that this conviction resulted from an investigation conducted by the Delphos (Ohio) Police Department. According the records, JASON BIGLER traveled to the City of Delphos to engage in sexually explicit conduct with a 14-year old girl who he met on a teen Internet chat line and who he communicated with via the Yahoo messenger application.
  - c. In June 2007, JASON BIGLER was convicted in the United States District Court for the Southern District of Ohio of one count of possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(b) & (b). JASON BIGLER was sentenced to 120 months imprisonment and lifetime supervised release. Based on records obtained from prior FBI case reports, I have determined that this conviction resulted from an investigation conducted by the FBI and Adult Parole Authority. Records identified that after JASON BIGLER was released from prison for his 2002 conviction and while he was serving a term of parole, Parole Officers found him in possession of various computer media. Possessing this computer media was a violation of his parole conditions, and the computer media were seized and examined. The examination recovered approximately 190 images and approximately 12 videos of child pornography.
92. JASON BIGLER was released from federal prison on or around December 2, 2014, and he is presently serving his term of lifetime supervised release. He is currently supervised by Probation Officer (PO) Christopher Owens of the United States Probation Service in Dayton, Ohio. As part of the conditions of his supervised release, JASON BIGLER is prohibited from possessing or using a computer or any device with access to any “on-line computer service” at any location without prior written approval of his probation officer. PO Owens has not provided such approval to JASON BIGLER. As such, JASON BIGLER is prohibited from having email and Dropbox accounts and accessing Internet data from his cellular telephone, tablet, and other electronic devices.
93. JASON BIGLER has reported to PO Owens that he resides at 105 Virginia Avenue in Dayton, Ohio. PO Owens’ records indicate that JASON BIGLER began living at this address in or around January 2015. Pursuant to the terms of JASON BIGLER’s

supervised release, PO Owens has conducted multiple home visits at 105 Virginia Avenue in Dayton, Ohio, and has confirmed that JASON BIGLER resides at this address. As part of his sex offender registration requirements, JASON BIGLER has also reported to the Montgomery County (Ohio) Sheriff's Office that he resides at 105 Virginia Avenue in Dayton, Ohio.

94. JASON BIGLER has told PO Owens that his telephone number is 937-304-4995 (the telephone number noted in the subscriber information for the bigblue8992@yahoo.com and bigblue8992@gmail.com email accounts, as detailed above). PO Owens has communicated with JASON BIGLER via this telephone number on numerous occasions.
95. JASON BIGLER has reported to PO Owens that he drives a 2000 Saturn SL1 bearing Ohio license plate AXN4197, silver in color. During previous home visits, PO Owens has seen JASON BIGLER drive the Saturn and/or has seen the vehicle parked in front of or near the residence at 105 Virginia Avenue.
96. I have determined that JASON BIGLER's residence at 105 Virginia Avenue in Dayton, Ohio is located directly across the street from Lois Bigler's residence at 104 Virginia Avenue in Dayton, Ohio (where Internet Service is received via Cincinnati Bell). Based on my training and experience, I know that Internet service for a residence can often be accessed from neighboring residences. Based on the proximity of the two residences located at 104 Virginia Avenue and 105 Virginia Avenue, JASON BIGLER could likely access Lois Bigler's Internet service from computer media at his residence and/or could easily travel to Lois Bigler's residence to use her computer media.

#### Execution of Search Warrants for Residences and Vehicle

97. On February 17, 2017, the United States District Court for the Southern District of Ohio authorized search warrants for the following:
  - a. The residential property located at 104 Virginia Avenue, Dayton, Ohio, 45410 (Lois Bigler's residence);
  - b. The residential property located at 105 Virginia Avenue, Dayton, Ohio, 45410 (JASON BIGLER's residence);
  - c. A 2000 Saturn SL1 bearing Ohio license plate AXN4197, silver in color (JASON BIGLER's vehicle).
98. Agents and officers of the FBI and Dayton Police Department executed the aforesaid search warrants on February 21, 2017. Among other items, an iPad was seized from 105 Virginia Avenue; an Apple All-in-One computer was seized from 104 Virginia Avenue, and a Motorola cellular telephone was seized from the Saturn.
99. During the execution of the search warrant for 104 Virginia Avenue, agents encountered Lois Bigler and Donald Bigler. Lois Bigler and Donald Bigler consented to be



interviewed. In summary, Lois Bigler and Donald Bigler provided the following information (among other information):

- a. Lois Bigler and Donald Bigler resided at 104 Virginia Avenue. JASON BIGLER was Lois Bigler's and Donald Bigler's son, and he resided at 105 Virginia Avenue.
  - b. JASON BIGLER came over to Lois Bigler's and Donald Bigler's residence a few times per week to use their Apple All-in-One computer.
  - c. Lois Bigler had given JASON BIGLER her iPad approximately one year ago.
100. During the execution of the search warrants for 105 Virginia Avenue and the 2000 Saturn SL1, agents encountered JASON BIGLER. After being advised of his Miranda rights, JASON BIGLER consented to be interviewed. In summary, JASON BIGLER provided the following information (among other information):
- a. JASON BIGLER resided at 105 Virginia Avenue, and his parents resided at 104 Virginia Avenue.
  - b. The Motorola cellular telephone seized from the Saturn was his telephone. The telephone number for this device was 937-304-4995 (the telephone number noted in the subscriber information for the bigblue8992@yahoo.com and bigblue8992@gmail.com email accounts, as detailed above).
  - c. JASON BIGLER used the Apple All-in-One computer at his parents' residence to conduct Internet searches, send and receive emails, and help his parents with various computer activities. He also currently had Lois Bigler's iPad in his house. JASON BIGLER had used the iPad for the past approximately one and a half years to play games and check his email accounts.
  - d. JASON BIGLER initially denied that he could access his parents' wireless Internet service from his residence. JASON BIGLER later acknowledged that he could in fact access the Internet service from his residence and had done so on a number of occasions.
  - e. JASON BIGLER used the email addresses bigday@zoomtown.com, bigblue8992@yahoo.com, and bigblue8992@gmail.com.
  - f. When asked if he used any Dropbox accounts, JASON BIGLER responded that he did not want to answer the question. When asked if he had viewed child pornography on any of the computer devices, JASON BIGLER again responded that he did not want to answer the question. JASON BIGLER terminated the interview shortly thereafter.

101. A preliminary examination has been conducted of the iPad collected during the search of JASON BIGLER's residence. The examination provided the following information:
- The examination determined that the device was an iPad 4. As noted above, Dropbox Inc.'s records identified that an "iPad3,4" was linked to the bigblue8992@gmail.com and bigblue8992@yahoo.com Dropbox accounts.
  - Approximately 15 bookmarks were saved on the Internet browser for the device that appeared to be Dropbox sharing links. Two of the titles for these links were "Dropbox - Kids" and "Dropbox - LuvLittles Secret Stash". Based on my training and experience, these titles are consistent with sharing links that may contain child pornography or other content involving children.
  - No child pornography files were saved on the device.
102. On April 25, 2017, I attempted to access each of the fifteen sharing links that were saved as bookmarks on the iPad used by JASON BIGLER. I found that eight of these sharing links were no longer active. The remaining seven sharing links primarily contained images and videos of children, teenagers, and young adults in various states of undress, some of whom were engaged in sexually explicit conduct. At least approximately four of the sharing links contained one or more image or video files depicting child pornography (as defined by 18 U.S.C. § 2256). It should be noted that the content of these sharing links could have changed since the time that JASON BIGLER last accessed the files.
103. The examination of the Apple All-in-One computer collected during the search of Lois Bigler's and Donald Bigler's residence has not been completed at this time.

Search for Social Media Accounts

104. On May 1, 2017, I searched a law enforcement portal that identifies Facebook accounts associated with email addresses. Records from this portal identified that the email addresses bigblue8992@yahoo.com and amandabigs@yahoo.com were associated with two Facebook accounts. Based on this and other information noted in the Affidavit, I believe that JASON BIGLER is the user of these two Facebook accounts.
105. Also on May 1, 2017, I searched publicly available content of the Twitter website for accounts associated with the name "bigblue8992". I located an account with an account name of @bigblue8992, located at https://www.twitter.com/bigblue8992. I noted that the name "Jay" appeared in the header section of the account's homepage. The homepage also identified that the user had joined Twitter in October 2016. The homepage identified that the account was opened in October 2016, the user did not have any current tweets, the user was following two other users, and one individual was following the user. Based on this and other information noted in the Affidavit, I believe that JASON BIGLER is the user of the @bigblue8992 Twitter account.



106. I also searched publicly available content of the Instagram website for the account name **bigblue8992**. I located an account at the URL <https://www.instagram.com/bigblue8992>. I noted that a picture of JASON BIGLER, as well as the name "bigblue8992", appeared on the account's homepage. The homepage identified that the user had four followers, was following eight users, and had one post. Based on this and other information noted in the Affidavit, I believe that JASON BIGLER is the user of the **bigblue8992** Instagram account.

Evidence Available in Email and Social Media Accounts

107. In my experience, individuals involved in child pornography and child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via email, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
108. Also in my experience, individuals involved in child exploitation schemes often utilize social media accounts and dating websites as a means to locate and recruit victims. They then use email accounts and chat functions from the websites to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents. As detailed above, Jason Bigler purportedly used Internet communications to communicate with victims in 2000 and 2002.
109. Based on my training and experience, I know that individuals involved in child pornography offenses often trade images with each other via a variety of means, including email. Such individuals may share images and videos they have produced as well as images and videos obtained from others. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
110. As noted above, I know based on my training and experience that individuals involved in child exploitation offenses often utilize multiple accounts, aliases, and means to communicate about child exploitation offenses and obtain child pornography. Jason Bigler's possible use of the nicknames "Big Jay" and "J Big" the email address **amandabigs@yahoo.com** are consistent with such aliases.
111. I also know that many email, social media accounts, and Internet websites require users to provide their email account when registering for the accounts. The email, social media, and Internet providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. These messages can provide material evidence in cases

- involving child exploitation offenses because they help in identifying what social media and Internet accounts were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
112. Again in my experience, I know that individuals often have financial, telephone, and other account statements sent to them via their email accounts. These documents can help in establishing the identity of the email account user.
113. Also as noted above, email and social media providers maintain various subscriber and user information that its users provide when registering for its accounts. Such information is materially important in cases where email accounts are utilized to commit child exploitation offenses, as this information can help in confirming the identity of the individuals using the accounts and committing the offenses.
114. Email and social media providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

#### Conclusion on Probable Cause

115. Based on all of the information noted above, I believe that JASON BIGLER is the user of the following accounts: (1) bigblue8992@yahoo.com Dropbox account; (2) bigblue8992@gmail.com Dropbox account; (3) bigblue8992@yahoo.com email address; (4) bigblue8992@gmail.com email address; (5) amandabigs@yahoo.com email address; (6) bigblue8992@yahoo.com Facebook account; (7) amandabigs@yahoo.com Facebook account; (8) @bigblue8992 Twitter account, and (9) bigblue8992 Instagram account. I submit that there is probable cause to believe that:
- a. JASON BIGLER used the bigblue8992@yahoo.com and bigblue8992@gmail.com Dropbox accounts to possess, transport, distribute, and advertise child pornography – all of which was done while he was required to register as a sex offender.
- b. The aforesaid nine accounts contain evidence of JASON BIGLER's child pornography activities.

#### ELECTRONIC COMMUNICATIONS PRIVACY ACT

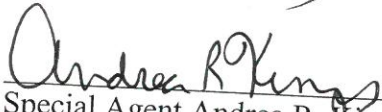
116. I anticipate executing the requested warrants for the listed accounts under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Yahoo Inc., Facebook Inc., Twitter Inc., and Instagram LLC to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Sections I of Attachments B-1 through B-4. Upon receipt of the information described in



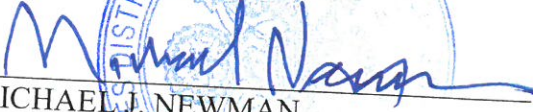
Sections I of Attachments B-1 through B-4, government-authorized persons will review that information to locate the items described in Sections II of Attachments B-1 through B-4.

**CONCLUSION**

117. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the accounts described in Attachments A-1 through A-4: advertisement of child pornography, in violation of 18 U.S.C. § 2251(d); receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1) and 2252A(a)(2); transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1); possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) and 2252A(a)(5)(B); and committing a felony offense involving a minor while being required to register as a sex offender, in violation of 18 U.S.C. § 2260A.
118. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-4.
119. Because the warrants for the accounts described in Attachments A-1 through A-4 will be served on Yahoo Inc., Facebook Inc., Twitter Inc., and Instagram LLC, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

  
Special Agent Andrea R. Kinzig  
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me  
this 22nd of May 2017

  
MICHAEL J. NEWMAN  
UNITED STATES MAGISTRATE JUDGE